

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

BRENT HOOTON,

Defendant.

No. 2:21-cr-00105-DAD-1

ORDER DENYING DEFENDANT'S
MOTION TO SUPPRESS

(Doc. No. 51)

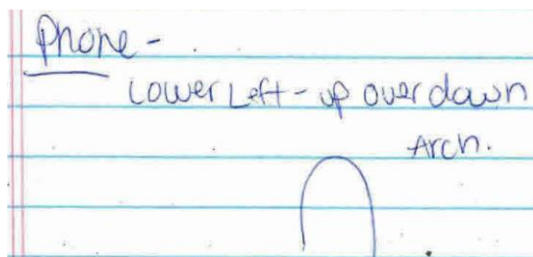
This matter is before the court on defendant Brent Hooton's motion to suppress evidence discovered during a search warrant executed at his residence on May 21, 2021, including his statements and the contents of his cell phone, pursuant to the Fourth, Fifth, and Sixth Amendment to the U.S. Constitution. (Doc. No. 51 at 1.)¹ A hearing on defendant's motion was held on May 18, 2023, at which Assistant United States Attorney Audrey Benison Hemesath appeared on behalf of the government, and Kresta Nora Daly appeared on behalf of defendant. For the reasons set forth below, the court will deny defendant Hooton's motion to suppress evidence.

////

¹ Although defendant states in his motion that he is moving to suppress evidence based on a violation of the Fourth Amendment (Doc. No. 51 at 1), he has advanced no argument to that effect in his briefing on the pending motion or at the hearing. Accordingly, the court will not address any potential Fourth Amendment-based contention in addressing defendant's motion to suppress evidence.

BACKGROUND

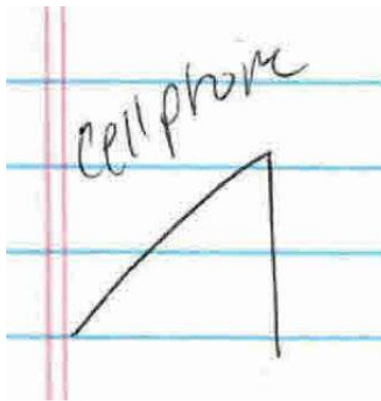
On May 20, 2021, the government filed a criminal complaint against defendant charging him in one count of sexual exploitation of a child for production of child pornography in violation of 18 U.S.C. § 2251(a) and one count of distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2). (Doc. No. 1.) That same day, the government sought and obtained a search warrant authorizing a search of defendant's residence for evidence related to the production and distribution of child pornography, which included a search of computers and mobile phones. (Doc. No. 55 at 1–2.) The following day, the government executed that search warrant and interviewed defendant without a lawyer on his behalf being present. (Doc. No. 51 at 3, 4.) Defendant initially consented to be interviewed after being advised of his *Miranda* rights and signing a standard waiver of rights form. (Doc. No. 55 at 2.) During that initial interview, defendant provided an alphanumeric password to his work computer, which granted access to defendant's work computer when it was tested later that day. (*Id.*) Defendant also visually demonstrated the pattern passcode to his Samsung Galaxy cell phone by moving his thumb through the air and by providing a description of that pattern passcode. (*Id.*) The pattern started in the lower left corner, then went up, over to the right, and then down. (*Id.*) Defendant Hooton's cell phone was not with him in the interview room; therefore, he described the password pattern without having his phone in front of him. (*Id.*) The interviewing agent documented her understanding of what defendant drew in the air as follows:



(*Id.* at 2.) Shortly after this discussion of his device passwords, defendant invoked his right to counsel. (*Id.*) The FBI agents then ceased their questioning of defendant and terminated the interview. (*Id.*) However, before transporting defendant to the Sacramento County Main Jail for booking, the FBI returned defendant to his residence for two reasons: (1) to obtain his

eyeglasses; and (2) to clarify his cell phone password that he had provided officers prior to his invocation of his right to counsel. (*Id.* at 3.)

At his residence, government agents made further inquiry about defendant's cell phone password. (Doc. No. 51 at 5.) Defendant Hooton then unlocked the cell phone and showed the interviewing agent the pattern. (Doc. No. 55 at 3.) Rather than an arch, the pattern password divulged by defendant at that time turned out to be angular, but it proceeded in the same general direction that defendant had described before invoking his right to counsel. (*Id.*) The agent drew the working pattern passcode in her interview notes as follows:



(*Id.* at 4.)

Defendant filed the pending motion to suppress evidence on April 24, 2023. (*Id.*) The government filed an opposition on May 8, 2023, and defendant filed his reply thereto on May 15, 2023. (Doc. Nos. 55, 59.)

ANALYSIS

A. Sixth Amendment

Defendant argues that law enforcement violated his Sixth Amendment right to counsel by interviewing him on May 21, 2021. (Doc. No. 51 at 3.)

The Sixth Amendment right to counsel prohibits the use of a criminal defendant's incriminating statements at trial where the police deliberately elicit the statements in the absence of the defendant's attorney. *Massiah v. United States*, 377 U.S. 201, 205–06 (1964). However, that right does not attach until “the initiation of adversary judicial criminal proceedings—whether by way of formal charge, preliminary hearing, indictment, information, or arraignment.” *Texas v.*

1 *Cobb*, 532 U.S. 162, 167–68 (2001) (quoting *McNeil v. Wisconsin*, 501 U.S. 171, 175, (1991));
 2 *see also Davis v. United States*, 512 U.S. 452, 456–57 (1994) (“[B]efore [adversary criminal]
 3 proceedings are initiated a suspect in a criminal investigation has no constitutional right to the
 4 assistance of counsel.”). The Ninth Circuit has explained that, because “a police inspector filing a
 5 complaint seeking an arrest warrant is not a critical stage that commits the prosecutor to trial,” no
 6 right to counsel attaches at arrest. *Anderson v. Alameida*, 397 F.3d 1175, 1180 (9th Cir. 2005).
 7 Similarly, a defendant’s Sixth Amendment right to counsel “[does] not attach upon the filing of
 8 the complaint by the FBI, the issuance of the warrant of arrest, or [the defendant’s] arrest.”
 9 *United States v. Pace*, 833 F.2d 1307, 1312 (9th Cir. 1987).

10 Here, defendant Hooton has not established that his Sixth Amendment right to counsel
 11 had attached at the time the agents spoke with him. Defendant’s statements which are at issue
 12 were made by him on May 21, 2021, the day of his arrest. At that point, adversarial judicial
 13 proceedings had not yet commenced; no preliminary hearing or arraignment had occurred, and no
 14 indictment had been returned. Thus, the admission of defendant’s statements on May 21, 2021
 15 could not violate his Sixth Amendment right to counsel because the time when those statements
 16 were made cannot be said to have been a “critical stage” of the prosecution, and thus defendant’s
 17 Sixth Amendment right to counsel had not yet attached. *See Cobb*, 532 U.S. at 167–68; *Pace*,
 18 833 F.2d at 1312; *Anderson*, 397 F.3d at 1180.

19 **B. Fifth Amendment *Miranda* Rights**

20 Defendant also argues that law enforcement violated his *Miranda* rights by questioning
 21 him about his cell phone password after he had asked for an attorney. (Doc. No. 51 at 5.)

22 In *Miranda v. Arizona*, 384 U.S. 436, 469–73 (1966), the Supreme Court held that
 23 individuals subject to custodial interrogation have the right to have counsel present during
 24 questioning, and police must inform them of this right before beginning questioning. Individuals
 25 may waive their *Miranda* rights after being advised of those rights. *Edwards v. Arizona*, 451 U.S.
 26 477, 484 (1981). If, however, an individual invokes their right to counsel, “the interrogation must
 27 cease until an attorney is present.” *Miranda*, 384 U.S. at 474. A court may only admit the
 28 defendant’s responses to further questioning if it finds that the defendant “initiated further

1 discussions with the police” and “knowingly and intelligently waived the right he had invoked.”
2 *Smith v. Illinois*, 469 U.S. 91, 95 (1981). “[A] valid waiver of that right cannot be established by
3 showing only that he responded to further police-initiated custodial interrogation even if he has
4 been advised of his rights.” *Edwards*, 451 U.S. at 484. “If the interrogation continues without
5 the presence of an attorney and a statement is taken, a heavy burden rests on the government to
6 demonstrate that the defendant knowingly and intelligently waived his privilege.” *Miranda*, 384
7 U.S. at 475. This rule is “designed to prevent police from badgering a defendant into waiving his
8 previously asserted *Miranda* rights.” *Michigan v. Harvey*, 494 U.S. 344, 350 (1990).

9 In this case, defendant was provided *Miranda* warnings, and he initially waived his rights
10 and voluntarily responded to the agent’s questions. (Doc. No. 55 at 2.) He then invoked his right
11 to counsel one hour into the interview, and the agents ceased the interrogation. (*Id.*) However,
12 defendant was then taken back to his house to retrieve his glasses, where there was a further
13 exchange between himself and the agents regarding the password to his cell phone that he had
14 provided prior to his invocation of his right to counsel. (*Id.* at 3, 5.) The government argues
15 that—even assuming that the agents violated defendant’s *Miranda* rights by further questioning
16 him about his cell phone password swipe pattern after defendant asked for an attorney—the
17 inevitable discovery doctrine prevents suppression of the evidence attained from the cell phone
18 search. (*Id.* at 4, 6.)²

19 “[T]he inevitable discovery doctrine allows for the admission of evidence that would have
20 been discovered even without the unconstitutional source.” *Utah v. Strieff*, 579 U.S. 232, 238
21 (2016) (citing *Nix v. Williams*, 467 U.S. 431, 443–44 (1984)). For the inevitable discovery
22 exception to apply, the prosecution must “establish by a preponderance of the evidence that the
23 information ultimately or inevitably would have been discovered by lawful means.” *Nix*, 467
24 U.S. at 444. “[I]nevitability discovery involves no speculative elements but focuses on
25 demonstrated historical facts capable of ready verification or impeachment.” *Id.* at 444 n.5.

26
27 ² The court notes that the government requested that the court decide the pending motion solely
28 based upon its assertion of the inevitable discovery doctrine and to assume, without deciding, that
a *Miranda* violation had occurred. The court will accept that request.

1 A number of courts have found that where law enforcement has the technological
2 capabilities to bypass a phone lock screen, the inevitable discovery doctrine applies, and evidence
3 obtained by the subsequent search of the cell phone should not be suppressed. *See United States*
4 *v. Coleman*, 554 F. Supp. 3d 1124, 1157 (D.N.M. 2021) (declining to suppress the contents of a
5 Galaxy phone under the doctrine of inevitable discovery, explaining “the likelihood that federal
6 agents would have and could have discovered the contents of the Galaxy cell phone evidence
7 pursuant to a valid warrant is high,” relying on testimony that Homeland Security Investigations
8 software would likely have accessed the contents of the Galaxy phone); *United States v. Todd*,
9 No. 4:16-cr-00305, 2017 WL 1197849, at *13 (S.D. Ga. Feb. 10, 2017), *report and*
10 *recommendation adopted*, No. 4:16-cr-00305, 2017 WL 1172113 (S.D. Ga. Mar. 29, 2017)
11 (declining to suppress the evidence obtained from a cell phone search, finding that the inevitable
12 discovery doctrine applied because the FBI had the technological capabilities to bypass the swipe
13 pattern); *United States v. Will*, No. 5:15-cr-00006, 2015 WL 3822599, at *16 (N.D. W. Va. June
14 19, 2015) (applying the inevitable discovery doctrine to deny a motion to suppress evidence,
15 finding that the officers possessed the technology to access the phone’s contents without a
16 password); *cf. United States v. Booker*, 561 F. Supp. 3d 924, 934–35 (S.D. Cal. 2021) (finding
17 that the government failed to satisfy its burden of demonstrating that the discovery of information
18 on the defendant’s cell phone fell within the inevitable discovery exception because the
19 technology for unlocking the particular cell phone at issue was not available when the
20 government extracted the contents of the phone and that the government provided no details
21 about the success rate associated with subsequently developed forensic tools).

22 Here, the government argues that the FBI could have easily bypassed defendant’s
23 Samsung Galaxy swipe pattern and that the FBI’s forensic tools were clearly capable of breaking
24 the code within one business day or less. (Doc. No. 55 at 6.) In support of its argument, the
25 government submitted the declaration of FBI digital forensics examiner Tanya Konrad, who
26 stated therein:

27 In my training and experience, Samsung Galaxy phones with
28 Android operating systems, particularly ones that use a pattern
passcode such as the cell phone in question here, are among the

1 easiest to unlock with Cellebrite digital forensic tools. Because the
2 pattern passcodes are limited in the number of possible numeric
3 combinations they can make, this relative lack of sophistication in
4 the passcode allows the digital forensic tool to quickly run through
5 all the possible passcodes that the user has selected. The cell phone
6 at issue would have been particularly easy to unlock because it only
7 had a 5-point pattern passcode, out of a possible 9-point pattern
8 passcode. In my training and experience, I estimate that it would
9 have taken in the proximity of 1 minute to 6 hours to unlock the
10 passcode of defendant's device using the Cellebrite digital forensic
11 tools available in May and June 2021.

12 (Doc. No. 55-1 at 50.) Furthermore, Ms. Konrad stated in her declaration that she had conferred
13 with Cellebrite technical support representatives and that they confirmed that in June 2021,
14 "Cellebrite Premium version 7.16.1.1 was capable of unlocking Samsung Galaxy phones with
15 Android operating systems." (*Id.*) Ms. Konrad's declaration did not specify the success rate of
16 the technology. *See Booker*, 561 F. Supp. 3d at 934 (noting that the declaration upon which the
17 government relied "provide[d] no details about the forensic tools such as their success rate"). At
18 the hearing on the pending motion, the court noted this shortcoming of Ms. Konrad's declaration,
19 which in turn led the government to request an evidentiary hearing without objection from the
20 defense. At that evidentiary hearing, Assistant U.S. Attorney Hemesath asked Ms. Konrad,
21 "What level of confidence do you have that the FBI would have been able to unlock the cell
22 phone in 2021?" Ms. Konrad replied, "I have a hundred percent confidence we were going to be
23 able to unlock that device, that specific device." Ms. Konrad further testified that in her
24 experience, Cellebrite unlocks Android devices that have swipe pattern locks like the one used
25 here with a zero-failure rate. The court found Ms. Konrad's testimony, which was not in any
26 meaningful way called into question by defense counsel's cross-examination, to be wholly
27 credible.

28 In his reply, defendant contends that the government did not meet its burden of
demonstrating that it had a surefire way to unlock his phone. (Doc. No. 59 at 1–3) (citing *Booker*,
561 F. Supp. 3d at 933–34). Specifically, defendant cites several articles and blog posts that
document security vulnerabilities in Cellebrite's technology in April 2021. (*Id.* at 2 n.1–2, 3 n.3.)
For example, defendant points to a reported flaw in which using Cellebrite to unlock a device
could corrupt evidence on the device if certain malware was already on the user's phone. (*Id.* at

1 2.) Defendant repeated this argument at the hearing on the pending motion. However, defendant
2 has offered no evidence suggesting that his particular cell phone had this type of malware on it.
3 Indeed, at the evidentiary hearing, Ms. Konrad testified that there was no indication or reason to
4 believe that defendant's cell phone contained malware that would have prevented the FBI from
5 accessing its contents.

6 Based upon the testimony provided at the evidentiary hearing conducted in connection
7 with the pending motion, the court finds that the government has met its burden of establishing by
8 a preponderance of the evidence that the contents of defendant's cell phone would have inevitably
9 been discovered by investigating agents. Therefore, even assuming, without deciding, that law
10 enforcement violated defendant's *Miranda* rights by questioning defendant about his cell phone
11 swipe pattern passcode after he had invoked his right to counsel, the inevitable discovery doctrine
12 is applicable here and suppression of the evidence attained from the search of defendant's cell
13 phone is not appropriate.

14 CONCLUSION

15 For the reasons explained above, defendant's motion to suppress (Doc. No. 51) is denied.

16 IT IS SO ORDERED.

17 Dated: May 22, 2023

18 
UNITED STATES DISTRICT JUDGE